

## **REMARKS**

Applicant has carefully considered the Examiner's comments in the Office Action mailed November 9, 2005. Claims 1-14 remain pending in the application and claims 27-34 have been added. Amendments have been made to claim 1. Support for the new claims and claim amendments can be found, e.g., at page 13, lines 18-24; page 17, at line 13 - page 18, line 16; in Figures 4A-4C; and in Figure 10. No new matter has been added to the application. Applicant respectfully requests reconsideration and allowance of claims 1-14 and 27-34.

### **Claim Rejections**

Claims 1-4, 11-21, and 23-26 have been rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,957,185 to Labaton. Claims 15-21 and 23-26 have been cancelled without prejudice or disclaimer, thereby rendering the rejection moot with respect to these claims. Regarding claims 1-4 and 11-14, Applicant respectfully submits that the rejection is overcome.

Claim 1 recites, in part, a method of obstructing identity crimes including linking a list of at least two identity verifiers to at least one numerical identifier associated with a registered user, providing the list to the registered user, and enabling the registered user to associate a security message with one of the identity verifiers. The method further includes receiving a numerical identifier and an identity verifier from a requesting party who obtained the numerical identifier and the identity verifier from a transaction initiator. The method also communicates information to the requesting party indicating whether the received identity verifier is within the list of identity verifiers linked to the received numerical identifier and sends to the requesting party any security message associated with the received identity verifier to enable the requesting party to compare the security message with a transaction being conducted by the transaction initiator.

In contrast, Labaton does not disclose or suggest linking a list of at least two identity verifiers to at least one numerical identifier associated with the registered user. Rather, Labaton discloses providing seeds numbers to enable a device to calculate one password at any one time. Furthermore, Labaton does not disclose or suggest enabling a registered user to associate a security message with one of the identity verifiers. Moreover, Labaton does not disclose or suggest sending to the requesting party any security message associated with the received

identity verifier to enable the requesting party to compare the security message with a transaction being initiated by the transaction initiator. Rather, Labaton discloses that the requesting party receives from the verification system only the password itself to be read aloud, e.g., column 14, lines 6-12.

For at least these reasons, Labaton does not anticipate claim 1. Claims 2-4 and 11-13 depend from claim 1 and are allowable for at least the same reasons. Applicant respectfully submits that the rejection is overcome and request withdrawal of the rejection. Applicant does not otherwise concede the correctness of the rejection and reserves the right to make additional arguments if necessary.

Claim 14 recites, in part, a method of determining whether an identity verifier is required to be submitted in a particular transaction. The method includes obtaining a list of at least two identity verifiers and linking the list of identity verifiers to at least one numerical identifier. The method also includes creating categories of transactions and receiving instructions from the registered user designating the categories of transactions that require an identity verifier and designating the categories of transactions that do not require an identity verifier. The method further includes determining whether a transaction requires the use of an identity verifier.

Labaton does not disclose or suggest creating categories of transactions. Furthermore, Labaton does not disclose or suggest receiving instructions from a registered user designating which categories require an identity verifier and which categories do not require an identity verifier (e.g., a password). Rather, passwords are utilized in each of the transactions disclosed in Labaton. In particular, the passage from column 13, line 62 through column 15, line 60, which was used as support to reject each element of claim 14, does not disclose or suggest any transaction in which a password is not used. For example, a password is used when verifying the identity of the certification service, e.g., column 14, lines 3-24. A password is also used when verifying a hand-written signature on a document, e.g., column 15, lines 45-60. Most of the remainder of the passage discloses how the passwords are encrypted and decrypted. No motivation is provided in Labaton to enable a registered user to conduct some transactions without providing an identity verifier.

For at least these reasons, therefore, Labaton does not anticipate claim 14. Applicant respectfully submits the rejection is overcome and requests reconsideration and allowance of

claim 14. Applicant does not otherwise concede the correctness of the rejection and reserves the right to make additional arguments if necessary.

Claim 5 has been rejected under 35 U.S.C. 103(a) as being unpatentable over Labaton as applied to claim 1, and further in view of U.S. 6,047,281 to Kuhns et al. Applicant again respectfully points out that the Kuhns reference is U.S. patent number 5,224,173. The reference having U.S. patent number 6,047,281 is issued to Wilson et al., not to Kuhns et al. As discussed in the previous response, because columns 16 and 17 in the Wilson patent include only the claims, Applicant assumes that the Examiner meant to reject claim 5 over Labaton in view of U.S. Patent No. 5,224,173 to Kuhns. Applicant respectfully traverses the rejection.

Claim 5 depends from claim 1 and is allowable over Labaton for at least the same reasons as discussed above with respect to claim 1. Kuhns does not overcome the shortcomings of Labaton. Kuhns does not disclose or suggest enabling a registered user to associate a security message with one of the identity verifiers. Rather, Kuhns is directed towards determining whether a scanned fingerprint is already stored within a central database.

Kuhns discloses associating certain physical characteristics of a user with the user's fingerprint. However, even if a fingerprint can be considered equivalent to the numerical identifier of claim 1 and even if physical characteristics can be considered equivalent to identity verifiers of claim 1, a point applicant does not concede for at least the reasons discussed in the previous response, Kuhns still does not disclose enabling a registered user to associate a security message with an identity verifier. The physical characteristics of a user are not used for only one transaction. Rather, all physical characteristics can be used in all transactions. Furthermore, the registered user does not choose which physical characteristics are used to narrow down the fingerprint search. The registered user, therefore, cannot choose to associate a security message with one of the identity verifiers for use during a particular transaction.

For at least these reasons, Labaton would not lead a person having skill in the art to the invention of claim 5, even if view of Kuhns. Applicant respectfully submits that the rejection is overcome and requests reconsideration and allowance of claim 5. Applicant does not otherwise concede the correctness of the rejection and reserves the right to make additional arguments if necessary.

Claims 6 and 9 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Labaton as applied to claim 1, and further in view of U.S. 6,236,972 to Shkedy. Applicant respectfully traverses the rejection.

Claims 6 and 9 depend from claim 1 and are allowable over Labaton for at least the same reasons as discussed above with respect to claim 1. In addition, Labaton discloses using a device serial number as the numerical identifier. The numerical identifier in Labaton is used as an index key to access the seed numbers necessary to generate a password for a particular transaction. The numerical identifier, therefore, identifies the remote device and not the user. For example, if the remote device were transferred to another user, then the social security number of the first user would be meaningless. For at least these reasons, Labaton teaches away from using a social security number as the numerical identifier and cannot be combined with the teachings of Shkedy.

Shkedy does not overcome the shortcomings of Labaton. Shkedy is directed towards a system for buying and selling mutual funds. Shkedy does not disclose or suggest enabling a registered user to associate a security message with one identity verifier. In fact, Shkedy does not provide much disclosure regarding verifying the identity of the parties. One example of a verification process given in Shkedy includes performing a 512-bit NSA private key operation with a micro-controller. See, *e.g.*, col. 9, lines 20-32. Public and private key cryptographic processes are known in the art and differ widely from the claimed invention. For example, each private key in such a verification process corresponds with one public key. Shkedy, therefore, teaches away from using one of multiple identity verifiers to verify a numerical identifier.

For at least these reasons, Labaton would not lead a person having skill in the art to the invention of claims 6 and 9, even in view of Shkedy. Applicant respectfully submits that the rejection is overcome and requests reconsideration and allowance of claims 6 and 9. Applicant does not otherwise concede the correctness of the rejection and reserves the right to make additional arguments if necessary.

Claims 7, 8, and 10 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Labaton as applied to claim 1, and further in view of U.S. 6,796,494 to Gonzalo. Applicant respectfully traverses the rejection.

Claims 7, 8, and 10 each depend from claim 1 and are allowable over Labaton for at least the same reasons as discussed above with respect to claims 1. Furthermore, Applicant submits that claims 7, 8, and 10 are also allowable over Labaton for at least the same reasons as discussed above with respect to claims 6 and 9. Gonzalo does not overcome the shortcomings of Labaton. Gonzalo does not disclose associating a security message with an identity verifier. Gonzalo does not even disclose how a customer's identity is verified. Rather, Gonzalo discloses configuring a publicly available computer system using a card.

For at least these reasons, Labaton would not lead a person having skill in the art to the invention of claim 1, even in view of Gonzalo. Claims 7, 8, and 10 depend from claim 1 and are allowable for at least the same reasons. Applicant does not otherwise concede the correctness of the rejection and reserves the right to make additional arguments if necessary.

Claim 22 has been rejected under 35 U.S.C. 103(a) as being unpatentable over Labaton as applied to claim 20, and further in view of U.S. 5,770,844 to Henn. Claim 22 has been cancelled without prejudice or disclaimer, thereby rendering the rejection moot. Applicant does not otherwise concede the correctness of the rejection and reserves the right to make additional arguments if necessary.

### **New Claims**

Claim 27 recites, in part, a method of obstructing identity crimes including associating identity verifiers with a registered user, receiving from the registered user at least one security message, and associating each security message to a corresponding identity verifier. The method further includes receiving one of the identity verifiers from a requesting party, who received the identity verifier from a transaction initiator. The method transmits to the requesting party an indication of whether the identity verifier received from the requesting party is associated with a corresponding security message.

Labaton does not disclose or suggest receiving from the registered user a corresponding message to be associated with the identity verifier, associating the identity verifier with the corresponding message, and transmitting an indication of whether the identity verifier received from the requesting party is associated with a corresponding security message. Rather, in Labaton, the passwords are generated at the time of transaction (when the user pushes the button

to request a password). The user does not know the password before pushing the button. The user, therefore, cannot provide a security message to be associated with a specific password. Furthermore, the verification cannot associate such a security message with one particular password prior to be contacted by the requesting party.

For at least these reasons, Labaton does not anticipate claim 27. Claim 28 depends from claim 27 and is allowable for at least the same reasons. Applicant respectfully requests consideration and allowance of claims 27 and 28.

Claim 29 recites, in part, a method of protecting numerical identifiers associated with registered users. The method includes obtaining for each registered user at least two identity verifiers and a list including at least one numerical identifier. Each of the identity verifiers enables the registered user to verify to a requesting party a selected numerical identifier from the list in only one transaction, and each of the identity verifiers is capable of verifying the selected numerical identifier in the one transaction.

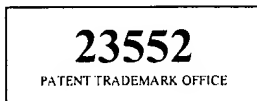
Labaton does not disclose or suggest obtaining for each registered user at least two identity verifiers that enable the registered user to verify to a requesting party a selected numerical identifier. Labaton further does not disclose or suggest that each identity verifier is capable of verifying the selected numerical identifier in the one transaction. Rather, the portable device disclosed in Labaton has a serial number and one or more seed numbers enabling the device to generate one password upon a request by the user. At any given time, only one particular password can be generated using the provided seed number. Only that password, therefore, can be used to verify the transaction.

For at least these reasons, Labaton does not anticipate claim 29. Claims 30-32 depend from claim 29 and are allowable for at least the same reasons. Applicant respectfully requests consideration and allowance of claims 29-32.

Claim 33 recites, in part, a system for protecting numerical identifiers of registered users. The system includes an input device, a database, and a communications device. Applicant respectfully submits that Labaton does not anticipate claim 33 for at least the same reasons as discussed above with respect to claim 29. Applicant respectfully requests consideration and allowance of claim 33.

Claim 34 recites, in part, a system of obstructing identity crimes. The system includes an input device, a database, a communication device, and a processing device. Applicant respectfully submits that Labaton does not anticipate claim 34 for at least the same reasons as discussed above with respect to claims 1 and 27. Applicant respectfully requests consideration and allowance of claim 34.

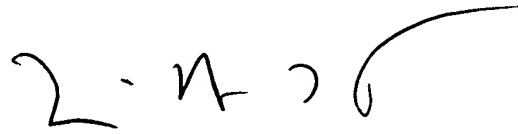
In view of the above amendments and remarks, Applicant respectfully requests a Notice of Allowance. If the Examiner believes a telephone conference would advance the prosecution of this application, the Examiner is invited to telephone the undersigned at the below-listed telephone number.



Respectfully submitted,

MERCHANT & GOULD P.C.  
P.O. Box 2903  
Minneapolis, Minnesota 55402-0903  
(612) 332-5300

Date: April 10, 2006

  
\_\_\_\_\_  
Brian H. Batzli  
Reg. No. 32,960